PERKINS COIE LLP
Susan D. Fahringer (Bar No. 162978)
SFahringer@perkinscoie.com
Nicola Menaldo (*Pro Hac Vice*)
NMenaldo@perkinscoie.com
Lauren J. Tsuji (Bar No. 300155)
LTsuji@perkinscoie.com
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000

Sunita Bali (Bar No. 274108)
SBali@perkinscoie.com
505 Howard Street, Suite 1000
San Francisco, California 94105-3204
Telephone: 415.344.7000
Facsimile: 415.344.7050

Attorneys for Defendants YouTube, LLC and Google LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

BRAD MARSCHKE, individually, and on behalf of all others similarly situated,

Plaintiff

v.

YOUTUBE, LLC and GOOGLE LLC,

Defendants.

Case No. 3:22-cv-06987-JD

DEFENDANTS' REPLY IN SUPPORT OF MOTION TO DISMISS AMENDED CLASS ACTION COMPLAINT

Judge: Hon. James Donato

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

STATUTES

I. INTRODUCTION

The facts alleged in the First Amended Complaint show that the privacy-protective features targeted by this case do two things, neither of which identify anyone, and neither of which violate the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.* ("BIPA"): *First*, Face Blur *prevents* individuals from being recognized, by identifying the shapes of objects in videos, then, if those shapes are faces, grouping and numbering them to enable the video uploader to apply blurring throughout the entire video. *Second*, Thumbnail Generator merely suggests still images from the uploaded video that the user can select as a video thumbnail. Nothing more. These features did not identify Marschke or anyone else whose face appears in videos uploaded to YouTube. And how could they, when these people necessarily include "total strangers" to the company"? *Zellmer v. Facebook, Inc.*, No. 3:18-cv-01880-JD, 2022 WL 976981, at *3 (N.D. Cal. Mar. 31, 2022).

In response, Marschke waxes poetic about a dystopian future, then repeats his conclusions—which are equally fictional—that Defendants violate BIPA. He erects strawmen, implying—incorrectly—that Defendants are arguing that people do not have a privacy right in connection with biometric data. And to sidestep the prohibition on applying BIPA extraterritorially and the requirement of aggrievement, Marschke points only to his *own* in-state conduct, and relies entirely on conclusory recitals, unsupported by facts.

Marschke never squarely contends with the most fundamental problem with his claims, which is that numbering similarly-shaped images of faces simply is not the same as "identifying" someone. Instead, he tries to equate the two. But BIPA's language is clear: *identification* is what matters. As in *Daichendt v. CVS Pharmacy, Inc.*, No. 22 CV 3318, 2022 WL 17404488 (N.D. Ill. Dec. 2, 2022), where the complaint was dismissed for failure to allege facts showing "the most foundational aspect of a BIPA claim"—i.e., that the data at issue identified, or were even capable of identifying, the plaintiff—Marschke's FAC should be dismissed. *Id.* at *5; *see also Wise v. Ring, LLC*, No. C20-1298-JCC, 2022 WL 3083068, at *3 (W.D. Wash. Aug. 3, 2022).

II. ARGUMENT

A. BIPA Does Not Apply to Face Blur and Thumbnail Generator, Which Do Not and Cannot Identify Anyone

Marschke concedes that to qualify as either a "biometric identifier" or "biometric information," data must—at a minimum—have the *capacity* to be used for identification, but argues that any "unique physical characteristic" satisfies this requirement. *See* Opp. at 2–3. His proposed interpretation of these terms is incorrect, but even under his expansive view of the statute, Marschke's FAC does not plausibly allege that Face Blur or Thumbnail Generator collect or use data that identify or can identify individuals who appear in videos uploaded to YouTube. *Id.* at 5.

1. "Biometric identifiers" and "biometric information" must identify a person.

Marschke suggests that the term "biometric identifier" means a "unique physical characteristic" that is "static and exclusive to a person, i.e., something that *can be used to identify* a unique individual." Opp. at 3 (emphasis added). According to Marschke, it follows that *any* "scan" of a face—whether complete or incomplete, whether used for identification or not—necessarily constitutes a "biometric identifier" under BIPA. But Marschke's proposed interpretation does not square with the statute's plain language, its structure, or its legislative history, and it is unsupported by the caselaw he cites.

First, Marschke does not even attempt to engage with the plain meaning of the term "identifier" which, as explained in Defendants' Motion, refers to data that *in fact "*identifies," i.e., "states the identity of (someone or something)." Mot. at 5; *see also* FAC ¶ 70 (recognizing that "specific individual facial recognition" is "critical" to liability under BIPA). Instead, Marschke suggests that because "biometric identifier" is defined to *include* a "scan of face geometry," no further analysis is needed. Opp. at 3. But reading the identification requirement out of "biometric identifier" as he urges would violate well-established canons of statutory construction that prohibit interpreting a statute in a way that would render portions of it superfluous. *See, e.g.*, *Kraft, Inc. v. Edgar*, 561 N.E.2d 656, 661 (1990). Had the Illinois General Assembly intended BIPA to apply to data whether or not it is in fact used to identify anyone, it easily could have omitted the reference to "identifiers" altogether—for example, by using terminology such as "biometric data," "biometric

input," or simply "biometrics." But it did not do so, and interpreting "biometric identifier" to cover data that does not identify anyone would render the term "identifer" superfluous and meaningless, in contravention of this well-established principle.

Second, instead of engaging with the Illinois General Assembly's motivation for adopting BIPA—which is entirely consistent with interpreting the term "biometric identifier" to require identification (*see* Mot. at 6)—Marschke broadly dismisses this legislative history as "irrelevant." *See* Plaintiff's Response to Defendants' Request for Judicial Notice, Dkt. No. 72 at 2. Of course, courts can and often do look to a statute's legislative history in ascertaining its meaning. *See, e.g.*, *Krohe v. City of Bloomington*, 204 Ill. 2d 392, 398 (2003) ("[A] statute's legislative history and debates are valuable construction aids in interpreting an ambiguous statute.") (cleaned up).

Third, unable to overcome the identification requirements inherent in the terms "biometric identifier" and "biometric information," Marschke selectively quotes from the caselaw to advance a position that it does not support. Opp. at 2–3. For example, Marschke relies on *Rivera v. Google, Inc.* 238 F. Supp. 3d 1088 (N.D. Ill. 2017), but omits that court's threshold finding that the data at issue there was, *in fact*, "*used* to identify a person." *Id.* at 1095. Likewise, Marschke's reliance on *Carpenter v. McDonald's Corp.*, 580 F. Supp. 3d 512 (N.D. Ill. 2022) and *Sosa v. Onfido, Inc.*, 600 F. Supp. 3d 859 (N.D. Ill. 2022), is unpersuasive because neither case turned on interpretation of the terms "biometric identifier" or "biometric information." In *Carpenter*, whether a "voiceprint" constituted a "biometric identifier" was not in dispute; rather, the question before the court was whether the plaintiff had adequately alleged collection of "voiceprints" in the first instance. 580 F. Supp. 3d at 516–18. And in *Sosa*, the court merely took it for granted that "faceprints" were "scans of face geometry and, therefore, 'biometric identifiers' under BIPA." 600 F. Supp. 3d at 871.

In short, Marschke has not provided any grounds for expanding the statute as he proposes.

2. Marschke does not plausibly allege that Face Blur and Thumbnail Generator identify, or even are capable of identifying, anyone.

Even if Marschke were correct that the terms "biometric identifier" and "biometric information" include data that merely *can be used* to identify a person, he does not plausibly allege that Defendants collect such data. Marschke concedes that Defendants do not link the alleged

"scans of face geometry" to identifying information such as his name or account number. *See* Opp. at 5–6. Instead of engaging with the arguments raised in Defendants' Motion, Marschke simply mischaracterizes these arguments, then repeats the same conclusory statements found in his FAC.

First, Marschke responds to an argument that Defendants did not make in suggesting that Face Blur and Thumbnail Generator need not "suggest any 'individual's name'" to violate BIPA. Opp. at 5. To be clear, the problem with Marschke's FAC is not that it fails to allege conduct identical to that at issue in *In re Facebook Biometric Information Privacy Litigation*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016) or *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017)—i.e., that the features recognize individual faces and link them to individual names. *See* Mot. at 8. The problem is that he fails to plausibly allege *any* facts suggesting that either Face Blur or Thumbnail Generator identify—or are capable of identifying—the individuals who appear in videos uploaded to YouTube, either by recognizing their faces or by linking face data to *any* type of identifying information.

Second, Marschke does not explain how the data he claims Face Blur and Thumbnail Generator collect can be used to identify anyone. Instead, he merely asserts that the FAC contains "well-pleaded facts" to this effect. Opp. at 6. As to Face Blur, he does not offer facts supporting his claim that "scan[s] of face geometry" allegedly captured by the feature can be used to do anything more than distinguish the faces that appear in a video from one another (i.e., by assigning a numerical "faceId" to the first face that appears in the video, a different numerical "faceId" to the second face that appears in the video, and so forth). Instead, he only speculates that a "faceId" is used to "personally identify[] the individuals selected." FAC ¶ 55; Opp. at 6. As to Thumbnail Generator, he offers no facts supporting his claim that the feature "scan[s], detect[]s, and collect[s] facial geometry," nor does he explain how the "face data" he alleges is "used to auto-generate thumbnails that contain faces, and especially faces with more expression" can be used or is used to identify an individual. FAC ¶ 66.

Because nothing in the FAC or the Opposition supports Marschke's conclusion that the data from either Face Blur or Thumbnail Generator is or can be used to identify a person, he has failed

to allege that it is actionable under BIPA.

3. Marschke's Proposed Non-User Class Makes This Case No Different from *Zellmer*.

Defendants' Motion cited *Zellmer v. Facebook, Inc.*, No. 3:18-cv-01880-JD, 2022 WL 976981 (N.D. Cal. Mar. 31, 2022), for the proposition that BIPA should not be construed to require companies to provide notice to and obtain consent from "non-users"—i.e., bystanders and others who appear in videos, but whose identities are unknown to Defendants. Mot. at 9 (quoting *Zellmer*, 2022 WL 976981, at *3). Instead of engaging with *Zellmer* at all, Marschke misleadingly suggests that this case is different because he "is a YouTube creator, and the proposed Class includes other such users." Opp. at 7. But Marschke's proposed class *also* includes non-users—specifically, "*every* Illinois resident who, while in Illinois, had their face appear in a video uploaded to YouTube from Illinois." FAC ¶ 91 (emphasis added). Nothing in the FAC limits the proposed class to users who themselves uploaded videos to YouTube, or used either Face Blur or Thumbnail Generator.

Marschke also suggests that *Zellmer* is inapposite because it was resolved at summary judgment, but there is no reason that its well-reasoned logic should not apply at Rule 12. Opp. at 7. The Court's analysis in *Zellmer* did not turn on the factual record—indeed, it acknowledged that there were unresolved "technical questions" as to whether the alleged face scans "were 'biometric identifiers' or 'biometric information' within the meaning of BIPA, and whether [defendant] 'collects' or 'possesses' the face scans." *Zellmer*, 2022 WL 976981, at *3. Instead, *Zellmer* relied on straightforward canons of statutory interpretation and legislative intent to find that the case presented an "untenable construction" of BIPA, which "would lead to obvious and insoluble problems" and "impose extraordinary burdens on businesses." *Id.* at *3–5. Here, as there, Marschke's proposed construction of the statute would require Defendants to identify every resident of Illinois and "figure out a way to communicate with them to provide notice and obtain consent," *before* they appear in a video uploaded to YouTube. *Id.* at *4. And, as there, "[h]ow this might work as a practical matter is entirely unclear." *Id.*

Because this Court has already concluded that BIPA cannot be applied to non-users, it can and should apply its own precedent, and dismiss the non-user claims from this case. *See also, e.g.*,

Fifth Third Bancorp v. Dudenhoeffer, 573 U.S. 409, 425 (2014) (Rule 12 is an "important mechanism for weeding out meritless claims").

B. Marschke Cannot Avoid Dismissal on Extraterritoriality Grounds by Relying Entirely on His Own Conduct

Marschke concedes that conduct must occur "primarily and substantially" in Illinois to be actionable under BIPA and that the relevant inquiry focuses on the "totality of the actions of both the plaintiff and the defendant" that give rise to the dispute. Opp. at 8. He points to the following allegations, which he contends constitute conduct on the part of Defendants occurring in Illinois: (1) Defendants "collected, captured, and used" his data in Illinois; (2) Defendants failed to make publicly available, and failed to comply with, retention and deletion guidelines in Illinois; and (3) Defendants made their services available worldwide. Opp. at 8. But each of these alleged facts are either irrelevant to the extraterritoriality analysis, conclusory, or both. Ultimately, Marschke's claim redounds to the fact that *he* is a resident of Illinois, and *he* uploaded videos to YouTube from Illinois.

First, Marschke's repeated recitals regarding the location of the alleged "collection," "capture," and "use" of his biometric data are conclusory, and turn entirely on his claim that *he* uploaded the relevant content from within Illinois. *See* FAC ¶¶ 15 ("Defendants' capture, and Defendants' use of these biometric identifiers or information of Plaintiff and all Class members all take place in the state of Illinois"); 50 ("The . . . collection, and use of such scans of face geometry all take place in the state of Illinois"); 83 ("[Plaintiff's] videos were . . . collected by Defendants within the state of Illinois, and used by Defendants in the state of Illinois"); 103 ("Defendants' collection and use of Plaintiff's . . . biometric identifiers took place within the state of Illinois."). Nowhere does Marschke offer any facts suggesting that the alleged collection, capture, and use of such data occur locally—for example, that the data was processed locally on the same device from which it is uploaded, or on nearby servers. Marschke's reliance on cases where courts concluded that plaintiffs plausibly alleged facts showing that the relevant conduct occurred primarily and substantially in Illinois is therefore misplaced. *Rivera*, for example, involved allegations that photographs were *automatically* uploaded from devices in Illinois. *See Rivera*, 238 F. Supp. 3d at

1090. Likewise, *In re Facebook Biometric Information Privacy Litigation* involved allegations that Facebook *automatically* enrolled individuals into a facial recognition program, that *automatically* extracted users' alleged biometric information from photographs and *automatically* tagged individuals who appeared in the photos by name. *See* Amended Complaint ¶¶ 26, 29, 64, *In re Facebook Biometric Info. Priv. Litig.*, No. 3:15-cv-03747-JD (N.D. Cal. Aug. 28, 2015), Dkt. No. 40. Here, in contrast, Marschke has not alleged that Face Blur automatically collected any information, or that Face Blur or Thumbnail Generator linked any images or shapes in videos to names or similar identifying information, so these cases do not help him at all.

Second, Marschke's suggestion that Defendants' failure to post or comply with a retention and deletion policy occurred in Illinois is a non sequitur, as he makes no effort to explain how the alleged *non-occurrence* of an event occurred in Illinois. *See* Mot. at 12; *McGoveran v. Amazon Web Servs., Inc.*, No. 1:20-cv-1399-LPS, 2021 WL 4502089, at *4 (D. Del. Sept. 30, 2021).

Third, Marschke's suggestion that Defendants intend their services to be used "around the world" (Opp. at 9) appears nowhere in the FAC, but in any event, nationwide or worldwide conduct is no substitute for conduct occurring in Illinois. *See, e.g.*, *Maui Jim, Inc. v. SmartBuy Guru Enters.*, 386 F. Supp. 3d 926, 939–40 (N.D. Ill. 2019) ("[A] plaintiff's claims are insufficient to state a claim under [state law] where, as here, the plaintiff 'exclusively offers evidence of . . . nationwide, as opposed to Illinois-specific, conduct.'") (citation omitted). Otherwise, the requirement for in-state conduct would easily be satisfied in most cases, even where a defendant does nothing beyond making its products and services available in Illinois.

This leaves only Marschke's own residence, but as multiple courts have made clear, allegations that turn on the location of the plaintiff alone are insufficient to establish that conduct occurred "primarily and substantially" in Illinois. *See, e.g.*, *McGoveran*, 2021 WL 4502089, at *4 (holding that a plaintiff's residency alone is insufficient for purposes of establishing that conduct occurred "primarily and substantially" in Illinois);[1] *Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp.

[1] Marschke's Statement of Recent Decision attaches *McGoveran*'s subsequent ruling on defendants' motion to dismiss the amended complaint and only confirms the insufficiency of the allegations here. *See* Dkt. No. 77. In *McGoveran*, the Section 15(b) claim survived a motion to dismiss where it was supported by specific allegations regarding defendants' activity in Illinois,

2d 752, 775 (N.D. Ill. 2008) (same); *see also Vance v. Microsoft Corp.*, No. C20-1082JLR, 2022 WL 9983979, at *6 (W.D. Wash. Oct. 17, 2022) (holding that claims were barred by extraterritoriality doctrine where the "relevant conduct"—"downloading, reviewing, and evaluating" a dataset allegedly comprised of biometric data—did not occur in Illinois).

C. The Dormant Commerce Clause Prohibits Applying BIPA to Conduct Outside Illinois.

While conceding that the dormant Commerce Clause prohibits a state from directly regulating conduct beyond its borders, Marschke mistakenly contends that his claims do not implicate this prohibition, again because *he* is a resident of Illinois, and *he* uploaded videos to YouTube from within Illinois. *See* Opp. at 12–13 ("Plaintiff's claims are based on his use, in Illinois, of [YouTube]."). But Marschke has not plausibly alleged a single fact suggesting any conduct by *Defendants* in Illinois—let alone conduct that violates BIPA.

Insofar as Marschke seeks to nevertheless hold Defendants liable for conduct occurring entirely outside of Illinois, this case is indistinguishable from *Sam Francis Foundation v. Christies, Inc.*, 784 F.3d 1320 (9th Cir. 2015). *See* Mot. at 12–13. And while Marschke incorrectly suggests that the Ninth Circuit's ruling in *National Pork Producers Council v. Ross*, 6 F.4th 1021 (9th Cir. 2021), *cert. granted,* 142 S. Ct. 1413 (2022) compels a different result (Opp. at 13), that case is readily distinguishable. At issue there was whether the dormant Commerce Clause precludes states from regulating entirely *in-state* conduct, where such regulations only incidentally affect out-of-state conduct. In relevant part, the Ninth Circuit held that "state laws that regulate only conduct in the state . . . do not have impermissible extraterritorial effects." 6 F.4th at 1029.[2] Here, unlike in

---

which were based on citations to materials published by defendants themselves. That court reviewed those materials and found them sufficient for extraterritoriality purposes. *See McGoveran v. Amazon Web Servs., Inc.*, No. 1:20-cv-1399-LPS, 2023 WL 2683553, at *10 (D. Del. Mar. 29, 2023)). In addition to those portions specifically cited in the court's order, the amended complaint also alleged significant additional details about defendants' purported activity in Illinois that go well beyond the conclusory and unsupported recitals in Marschke's FAC. *See, e.g.*, First Amended Complaint ¶¶ 108–34, *McGoveran v. Amazon Web Servs., Inc.*, No. 1:20-cv-1399-LPS, 2022 WL 3274152 (D. Del. Feb. 17, 2022).

[2] *Ross* was heard by the U.S. Supreme Court in October 2021, and Defendants acknowledge some uncertainty as to the precise parameters of the dormant Commerce Clause. Nevertheless, Marschke's suggestion, in a footnote, that the dormant Commerce Clause is approaching a "dead

Ross, Marschke's proposed application of BIPA would necessarily regulate conduct well beyond the borders of Illinois, because Marschke has not alleged *any* conduct by Defendants occurring in Illinois. Further, for the reasons discussed above in Section II.A.2, Marschke has not alleged facts showing that Defendants can even identify the people whose faces appear in videos uploaded to YouTube, much less evaluate their state of residency. Given the impossibility of determining residency *ex ante*, Defendants would need to seek consent from everyone, nationwide, to comply with Marschke's interpretation of BIPA.

Marschke's Opposition also fails altogether to engage with the inconsistencies between BIPA—as he would have it applied—and the statutory scheme governing the collection, storage, and use of biometric data in California. Mot. at 13. Instead, Marschke dismisses these concerns out of hand, claiming that by this logic, "no state could regulate a corporation headquartered out-of-state." Opp. at 13. This is plainly not the case, as states can and routinely do require out-of-state companies to comply with local regulations governing *in-state* conduct. The problem here is that Marschke seeks to apply BIPA to *out-of-state* conduct, and seeks to do so in a manner which would threaten Defendants—and other out-of-state companies—with potentially inconsistent regulations from other states. The dormant Commerce Clause prohibits both results. *See, e.g.*, *Healy v. Beer Inst.*, 491 U.S. 324, 336–37 (1989).

D. Marschke Has Not Alleged That He Is "Aggrieved" by a Violation of Section 15(a)

Marschke claims he is "aggrieved" by a violation of Section 15(a) because Defendants (1) failed to post a publicly available retention schedule and guidelines for permanently destroying such biometric identifiers and (2) retained his biometric data "after" he used Face Blur and Thumbnail Generator. Opp. at 15. There are several problems with his argument.

First, as explained in Defendants' Motion, Marschke does not allege that Defendants failed to comply with an *existing* retention and deletion policy as to his data, as he must to establish that

---

letter" and that *Healy* is limited to "price control or price affirmation statutes" (Opp. at 13) is pure speculation. Indeed, the United States filed an amicus brief in *Ross*, arguing that the extraterritoriality principle announced in *Healy* applies more broadly. *See* Brief for the United States as Amicus Curiae Supporting Petitioners at 17–19, *Nat'l Pork Producers Council v. Ross*, No. 21-2468, 2022 WL 2288169 (2022).

he is "aggrieved." *See* Mot. at 14–15. To the contrary, he repeatedly concedes that Defendants do not have such a policy at all. *See, e.g.*, FAC ¶¶ 80 ("YouTube's website does not have a written, publicly available policy identifying its biometrics retention schedule, nor guidelines for permanently destroying Illinois users' biometric identifiers when they are no longer needed."); 86 ("Because Defendants failed to develop or implement a BIPA-compliant data collection policy, Defendants therefore failed to comply with any BIPA-compliant policy . . . ."); *see also id.* ¶¶ 108–09. But the duty to publish a written policy is a duty owed to the public as a whole, not to him specifically, and so this gets him nowhere as to showing his own "aggrievement." *See, e.g.*, *Am. Sur. Co. v. Jones*, 51 N.E.2d 122, 125 (1943); *In re Facebook Biometric Info. Priv. Litig.*, 326 F.R.D. 535, 546 (N.D. Cal. 2018), *aff'd sub nom. Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019).

Second, while Marschke claims that Defendants retained his data "after" he used Face Blur and Thumbnail Generator (Opp. at 15), these allegations appear nowhere in the FAC. As to Face Blur, the FAC merely speculates that "scan[s] of face geometry" are stored "for a longer period of time, and possibly permanently"—as demonstrated by the fact that "when the 'Face Blur' tool is run multiple times on the same video, the previously stored result is provided to the user without actually rerunning the tool again." FAC ¶¶ 56–58. That Face Blur returns the same results when it is run on the same video, however, does not lend support to Marschke's claim that *any* biometric data is "stored" by the tool "after" it is used, let alone "permanently." And as to Thumbnail Generator, the FAC includes no allegations whatsoever as to improper retention.

III. CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court dismiss the FAC.

Dated: April 17, 2023

PERKINS COIE LLP

By: */s/ Susan D. Fahringer*
Susan D. Fahringer (Bar No. 162978)
Sunita Bali (Bar No. 274108)
Nicola Menaldo (*Pro Hac Vice*)
Lauren J. Tsuji (Bar No. 300155)

Attorneys for Defendants
YouTube, LLC and Google LLC